PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Francesco Caturano

XXXIV Cycle

Training and Research Activities Report – Third Year

Tutor: Simon Pietro Romano

Information

My name is Francesco Caturano. I graduated in Computer Science Engineering in 2018 at University Federico II of Napoli, with a Thesis entitled “Automated discovery of CoAP-enabled IoT devices”. The Thesis activity was carried out at NomadicLab, Ericsson Finland.

I am a third year ITEE PhD student at University Federico II of Napoli, belonging to the XXXIV cycle. My PhD fellowship type does not provide departmental funds. I conducted the research activity using external fundings coming from a GARR (Gruppo Armonizzazione Reti della Ricerca) scholarship, for the whole first year, as well as for the major part of the second year.

Currently, I am holder of a DIETI fellowship, which focuses on the topic “Automating penetration testing procedures through Reinforcement Learning”.

My tutor is Professor Simon Pietro Romano.

Study and Training activities

To complete the seminars credit requirements, the following seminars have been attended:

- Beyond Einstein Gravity: Dark Energy and Dark Matter as Curvature Effects
- Palo Alto Network Prima Access
- Robot Manipulation and Control
- La norma ISO 27001 e la sua contestualizzazione nel panorama normativo nazionale ed internazionale

They fit well with my research activity. In fact, I am dealing with the application of Reinforcement Learning techniques to automate the procedures of Web Application Penetration Testing. All the attended seminars are either about modeling complex dynamic systems to provide automation, or about practical applications in the cybersecurity field.

Research activity

My research activity revolves around two main topics:

- Security Automation and Virtualization.
- Artificial Intelligence for Security testing.

The first area focuses on the study of cutting-edge virtualization technologies that allow for the design of emulated attack scenarios. They help building complex virtualized environments, commonly known as “cyber ranges”, used for training purposes of security professionals.

At the beginning of the third year of PhD, I presented the paper “Capturing flags in a dynamically deployed microservices-based heterogeneous enivironment” at the IPTcomm 2020 Conference. Such paper tackles, from a practical point of view, some of the limitations that arise from the use of OS virtualization for cyber ranges instantiation platforms. The paper also proposes a solution that enables integration of different virtualization technologies to the discussed issues and provide a heterogeneous virtualized environment for cybersecurity training exercises.

The second area of research focuses on the development of intelligent methodologies to test Web Applications security, using a black-box approach. During the third year, the paper “Discovering Cross-Site Scripting vulnerabilities using a Multiobjective Reinforcement Learning environment”, was accepted for publication by Computers & Security (Elsevier).
It discusses a model that frames the behavior of a hacker as a sequential decision making problem, under uncertainty. The problem is seen as a Markov Decision Process and solved using Reinforcement Learning. The developed approach has been tested on a particular vulnerability exploit model, known as Cross-Site Scripting.
To the purpose, a novel Multiobjective Reinforcement Learning environment was developed. The term “Multiobjective” signifies that there are several optimization targets for the reinforcement learning agent to pursue.
In order to provide users with a practical tool, useful during actual penetration testing campaigns, the first result has been a Suggester, a semi-automated platform that recommends the best actions to a human in the loop. Such system has shown very good results in terms of accuracy, compared to state of the art XSS detection tools.
During the third year, several developments to the presented architecture allowed to produce a fully automated platform, creating a completely autonomous agent that is able discover Cross-Site Scripting flaws in a web application.

The short paper “Hacking Goals: a goal-centric attack classification framework” was presented at ICTSS 32ND IFIP International conference on testing software and systems.
In this paper a “goal-centric” methodology to classify attacks in terms of Hacking Goals (the objective that the penetration tester is pursuing), has been showed. Many works have addressed the attack taxonomy problem, by introducing different ways to classify attacks. Penetration testers perform their activity by focusing on goals rather than attack types.

Starting from this goal-oriented attack taxonomy, an ontology for web application penetration testing has been developed, with the same ontology being represented in the form of a knowledge graph. A system built on top of such an ontology allows to provide recommendations to a penetration tester, using predefined rules and an inference engine that outputs the most

promising attack paths. Such an approach allows to address the scalability of the previously described intelligent agent, which becomes an issue with growing action-state spaces.

Finally, a platform capable of creating datasets for web application penetration tests, has been developed. Such a platform is based on a toolset that allows to collect ethical hackers' actions, such as browser interactions as well as generated network traffic. An encouragement to the research in the field of machine learning applied to cybersecurity is supposed to come from the release of open source datasets of hacking exercises.

The paper “A Distributed Security Tomography Framework to assess the exposure of ICT Infrastructures to Network Threats” provides means to define cyber security indicators through an automated and repeatable measurement process. The efficiency of the presented methodology by testing it on real-world infrastructure facilities has been proved, discussing the results obtained in two different scenarios: a comparison of networks with different characteristics and a real-time monitoring of the defined metrics.

The activities conducted during the final PhD year contribute to the development of the so-called cybersecurity awareness. Such mission refers to how much end-users know about the cyber security threats, the risks they introduce as well as the security best practices to mitigate them. Opposing such increasing threat has become a necessity for companies as well as public administrations, in order to guarantee data protection, which is the assumption behind the trust that end-users build towards their services.
Penetration testing is one such activity that allows to periodically check network infrastructures‘ exposure to cyber attacks. The ISO 27001 standard requires penetration tests to be scheduled periodically, in order to quickly identify vulnerabilities and avoid them being exploited by real attackers. By introducing intelligent logic to the automated tools that perform penetration tests, a step towards a better management of the mentioned activities is taken. By conducting security assessments in an automated and accurate fashion, security experts can focus on mitigation techniques as well as work on robust countermeasures for ever-emerging cyber attacks.

Products

- BRIGNOLI, M. A., et al. A distributed security tomography framework to assess the exposure of ICT infrastructures to network threats. Journal of Information Security and Applications, 2021, 59: 102833.
- CATURANO, Francesco; PERRONE, Gaetano; ROMANO, Simon Pietro. Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment. Computers & Security, 2021, 103: 102204.

Conferences and Seminars

Università degli Studi di Napoli Federico II

- Conference name: IPTcomm 2020 (Principles, Systems and Applications of IP Telecommunications);
- Place: Virtual (originally Chicago)
- Dates: 13 – 15 October 2020
- Accepted paper: “Capturing flags in a dynamically deployed microservices-based heterogeneous enivironment”

- Conference name: ICTSS 32ND IFIP
- Place: Virtual
- Dates: 9-11 December 2020
- Accepted paper: “Hacking Goals: a goal-centric attack classification framework”

Student: Francesco Caturano **Tutor: Simon Pietro Romano** **Cycle XXXIV**
francesco.caturano@unina.it spromano@unina.it

	Credits year 1								Credits year 2								Credits year 3								
		1	2	3	4	5	6			1	2	3	4	5	6			1	2	3	4	5	6		
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Total
Modules	18	0,8	1,2	6	8	3	5	**24**	15	0	0	0	4	4	0	**8**	21	0	0	0	0	0	0	**0**	**32**
Seminars	13	0	0	0	0,8	6	0,2	**7**	6	0	0	0	0	0	0	**0**	12	0,8	0	0	0	0	3,6	**4,4**	**11**
Research	34	9,2	8,8	4	1,2	1	4,8	**29**	39	10	10	10	6	6	10	**52**	30	9,2	10	10	10	10	6,4	**56**	**137**
	65	10	10	10	10	10	10	**60**	60	10	10	10	10	10	10	**60**	63	10	10	10	10	10	10	**60**	**180**

Check	Year	Lecture/Activity	Type	Credits	Certification	Notes
30-70	3	Beyond Einstein Gravity: Dark Energy and Dark Matter as Curvature Effects	Seminar	0,3	x	
10-30	3	Robot Manipulation and Control	Seminar	0,5	x	
80-140	3	Palo Alto Network Prima Access	Seminar	3,2	x	
180	3	La norma ISO 27001 e la sua contestualizzazione nel panorama normativo nazionale ed internazionale	Seminar	0,4	x	